EXHIBIT A

IN THE CIRCUIT COURT FOR BALTIMORE COUNTY, MARYLAND

ANITA BEAUFORD
4410 Woodlea Ave.,
Baltimore, MD 21206

    Plaintiff

v.

THE JOHNS HOPKINS HOSPITAL, INC.
600 North Wolfe Street
Baltimore, MD 21287

    SERVE ON:
    Peter B. Mancino
    The Johns Hopkins Hospital
    1812 Ashland Ave., Ste. 300
    Baltimore, MD 21205

And

THE JOHNS HOPKINS HEALTH SYSTEM
CORPORATION
600 North Wolfe Street
Baltimore, MD 21287

    SERVE ON:
    Peter B. Mancino
    The Johns Hopkins Hospital
    1812 Ashland Ave., Ste. 300
    Baltimore, MD 21205

And

THE JOHNS HOPKINS UNIVERSITY
3400 North Charles Street
Baltimore, MD 21218

    SERVE ON:
    Arthur P. Pineau
    113 Garland Hall
    3400 North Charles Street
    Baltimore, MD 21218

Case No:
Class Action Complaint
Jury Trial Demanded

C-03-CV-23-000501

1

CLASS ACTION COMPLAINT

Plaintiff Anita Beauford ("Plaintiff"), on behalf of herself and all other similarly situated individuals (the "Class Members") against The Johns Hopkins Hospital, Incorporated The Johns Hopkins Health System Corporation, and The Johns Hopkins University (collectively "Defendants"), brings this action based upon personal knowledge of the facts pertaining to herself, and on information and belief as to all other matters, by and through the investigation of undersigned counsel.

NATURE OF THE ACTION

1.   This is a class action lawsuit brought on behalf of all Maryland residents who have accessed and used any website that Defendants own and operate, including www.hopkinsmedicine.org.

2.   Defendants aid employ, agree, and conspire with Facebook/Meta[1] to intercept communications sent and received by Plaintiff and Class Members, including communications containing protected medical information. Plaintiff brings this action for legal and equitable remedies resulting from these illegal actions.

JURISDICTION AND VENUE

3.   The Court has subject matter jurisdiction over this action. Md. Cts. & Jud. Proc. Code § 1-501.

4.   The Court has personal jurisdiction over Defendants because Defendants transact business in the State. Md. Cts. & Jud. Proc. Code § 6-103(b)(1).

---

[1] In October 2021, Facebook, Inc. changed its name to Meta, Inc. Unless otherwise indicated, Facebook, Inc. and Meta, Inc. are referenced collectively herein as "Facebook."

5.   Venue is proper because Defendants carry on regular business within this County. Md. Cts. & Jud. Proc. Code § 6-201.

THE PARTIES

Plaintiff Beauford

6.   Plaintiff Anita Beauford is an adult citizen of the State and is domiciled in Baltimore, Maryland.

7.   Plaintiff Beauford regularly uses the www.hopkinsmedicine.org website to book medical appointments and access the patient portal. She first began using the website for the above-stated purposes in approximately 2021. Plaintiff Beauford accesses the website using her smartphone. As described below, each time Plaintiff Beauford booked medical appointments, she disclosed medical information regarding her medical condition, history or treatment.

8.   Plaintiff Beauford also has an active Facebook account which she has maintained since 2013. Plaintiff Beauford accesses her Facebook account from multiple devices, including her laptop, smartphone, and desktop computer.

Defendant

9.   Defendant The Johns Hopkins Hospital Inc. is a registered nonprofit entity with its principal place of business in Maryland. As of September 2022, this Defendant reported revenue of approximately $2.1 billion. This Defendant offers a full range of medical services, including primary, inpatient and outpatient care, and treats thousands of patients each year.

10.   Defendant The Johns Hopkins Health System Corporation is a registered entity with its principal place of business in Maryland. This Defendant is affiliated with The Johns Hopkins Hospital, Inc.

11.   Defendant The Johns Hopkins University is a private, nonprofit university located in Baltimore, Maryland. This Defendant is affiliated with The Johns Hopkins Hospital, Inc.

12.   Pursuant to the systematic process described herein, Defendants assisted Facebook with intercepting Plaintiff's communications, including those that contained personally identifiable information, protected health information and related confidential information. Defendants assisted these interceptions without Plaintiff's knowledge, consent or express written authorization.

13.   By failing to receive the requisite consent, Defendants breached confidentiality and unlawfully disclosed Plaintiff's personally identifiable information and protected health information.

FACTUAL ALLEGATIONS

The Maryland Wiretap Act

14.   Maryland's Wiretap Act prohibits: (a) the interception or procurement of another to intercept any wire, electronic or oral communication; (b) the intentional disclosure of the contents of any wire, electronic or oral communication that the discloser knew or should have known was obtained through the interception of a wire, electronic or oral communication; and (c) the intentional use of the contents of any wire, electronic or oral communication that the discloser knew or should have known was obtained through the interception of a wire, electronic or oral communication. Md. Cts. & Jud. Proc. Code § 10-402.

15.   Any person who intercepts, discloses, or uses or procures any other person to intercept, disclose or use, a wire, electronic, or oral communication in violation of the Maryland's Wiretap Act is subject to a civil action for: (a) actual damages, not less than liquidated damages computed at the rate of $100/day for each violation or $1,000, whichever is higher; (b) punitive

damages; and (c) reasonable attorneys' fees and other litigation costs incurred. Md. Cts. & Jud. Proc. Code § 10-410.

16.   Under Maryland's Wiretap Act, "intercept" is defined as any "[a]ural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device." Md. Cts. & Jud. Proc. Code § 10-401(10).

17.   Under Maryland's Wiretap Act, "contents" is defined as "used with respect to any wire, electronic or oral communication, includes any information concerning the identity of the parties to the communication or the existence, substance, purport, or meaning of that communication." Md. Cts. & Jud. Proc. Code § 10-401(4).

18.   Under Maryland's Wiretap Act, "person" is defined as "any individual, partnership, association, joint stock company, trust or corporation." Md. Cts. & Jud. Proc. Code § 10-401(14).

19.   Under Maryland's Wiretap Act, "electronic communication" is defined as "[a]ny transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo-optical system." Md. Cts. & Jud. Proc. Code § 10-401(5)(i).

Defendants and Their Website

20.   Defendants offer a full range of medical services, including primary, inpatient and outpatient care.

21.   Defendants operate www.hopkinsmedicine.org, which is accessible on desktop computers.

Facebook's Platform and Business Tools

22.   Facebook describes itself as a "real identity platform,"[2] meaning users are allowed only one account and must share "the name they go by in everyday life."[3] To that end, when creating an account, users must provide their first and last name, along with their birthday and gender.[4]

23.   In 2021, Facebook generated $117 billion in revenue.[5] Roughly 97% of that came from selling advertising space.[6]

24.   Facebook sells advertising space by highlighting its ability to target users.[7] Facebook can target users so effectively because it surveils user activity both on and off its site.[8] This allows Facebook to make inferences about users beyond what they explicitly disclose, like their "interests," "behavior," and "connections."[9] Facebook compiles this information into a generalized dataset called "Core Audiences," which advertisers use to apply highly specific filters and parameters for their targeted advertisements.[10]

---

[2] Sam Schechner and Jeff Horwitz, *How Many Users Does Facebook Have? The Company Struggles to Figure It Out*, WALL. ST. J. (Oct. 21, 2021).

[3] FACEBOOK, COMMUNITY STANDARDS, PART IV INTEGRITY AND AUTHENTICITY, https://www.facebook.com/communitystandards/integrity_authenticity.

[4] FACEBOOK, SIGN UP, https://www.facebook.com/

[5] FACEBOOK, META REPORTS FOURTH QUARTER AND FULL YEAR 2021 RESULTS, https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx

[6] *Id.*

[7] FACEBOOK, WHY ADVERTISE ON FACEBOOK, https://www.facebook.com/business/help/205029060038706.

[8] FACEBOOK, ABOUT FACEBOOK PIXEL, https://www.facebook.com/business/help/742478679120153?id=1205376682832142.

[9] FACEBOOK, AD TARGETING: HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, https://www.facebook.com/business/ads/ad-targeting.

[10] FACEBOOK, EASIER, MORE EFFECTIVE WAYS TO REACH THE RIGHT PEOPLE ON FACEBOOK, https://www.facebook.com/business/news/Core-Audiences.

25.   Advertisers can also build "Custom Audiences."[11]   Custom Audiences enables advertisers to reach "people who have already shown interest in [their] business, whether they're loyal customers or people who have used [their] app or visited [their] website."[12] With Custom Audiences, advertisers can target existing customers directly, and they can also build "Lookalike Audiences," which "leverage[] information such as demographics, interests, and behavior from your source audience to find new people who share similar qualities."[13] Unlike Core Audiences, advertisers can build Custom Audiences and Lookalike Audiences only if they first supply Facebook with the underlying data. Advertisers can do so through two mechanisms: (a) by manually uploading contact information for customers; or (b) by utilizing Facebook's "Business Tools."[14]

26.   As Facebook puts it, the Business Tools "help website owners and publishers, app developers and business partners, including advertisers and others, integrate with Facebook, understand and measure their products and services, and better reach and serve people who might be interested in their products and services."[15] Put more succinctly, Facebook's Business Tools are bits of code that advertisers can integrate into their websites, mobile applications and servers, thereby enabling Facebook to intercept and collect user activity on those platforms.

---

[11] FACEBOOK, ABOUT CUSTOM AUDIENCES,
https://www.facebook.com/business/help/744354708981227?id=2469097953376494.
[12] FACEBOOK, AD TARGETING, HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, https://www.facebook.com/business/ads/ad-targeting.
[13] FACEBOOK, ABOUT LOOKALIKE AUDIENCES,
https://www.facebook.com/business/help/164749007013531?id=401668390442328.
[14] FACEBOOK, CREATE A CUSTOMER LIST CUSTOM AUDIENCE,
https://www.facebook.com/business/help/170456843145568?id=2469097953376494;
FACEBOOK, CREATE A WEBSITE CUSTOM AUDIENCE,
https://www.facebook.com/business/help/1474662202748341?id=2469097953376494.
[15] FACEBOOK, THE FACEBOOK BUSINESS TOOLS,
https://www.facebook.com/help/331509497253087.

27.   The Business Tools are automatically configured to capture certain data, like when a user visits a webpage, the webpage's Universal Resource Locator ("URL") and metadata, or when a user downloads a mobile application or makes a purchase.[16] Facebook's Business Tools can also track other events. Facebook offers a menu of "standard events" from which advertisers can choose, including what content a visitor views or purchases.[17] Advertisers can even create their own tracking parameters by building a "custom event."[18]

28.   One such Business Tool is the Facebook Tracking Pixel. Facebook offers this piece of code to advertisers, like Defendants, to integrate into their websites. As the name implies, the Facebook Tracking Pixel "tracks the people and type of actions they take."[19] When a user accesses a website hosting the Facebook Tracking Pixel, Facebook's software script surreptitiously directs the user's browser to send a separate message to Facebook's servers. This second, secret transmission contains the original GET request sent to the host website, along with additional data that the Facebook Tracking Pixel is configured to collect. This transmission is initiated by Facebook code and concurrent with the communications with the host website. Two sets of code are thus automatically run as part of the browser's attempt to load and read Defendants' websites—Defendants' own code and Facebook's embedded code.

---

[16] *See* FACEBOOK, FACEBOOK PIXEL, ACCURATE EVENT TRACKING, ADVANCED, https://developers.facebook.com/docs/facebook-pixel/advanced/; *see also* FACEBOOK, BEST PRACTICES FOR FACEBOOK PIXEL SETUP, https://www.facebook.com/business/help/218844828315224?id=1205376682832142; FACEBOOK, APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/.

[17] FACEBOOK, SPECIFICATIONS FOR FACEBOOK PIXEL STANDARD EVENTS, https://www.facebook.com/business/help/402791146561655?id=1205376682832142.

[18] FACEBOOK, ABOUT STANDARD AND CUSTOM WEBSITE EVENTS, https://www.facebook.com/business/help/964258670337005?id=1205376682832142; *see also* FACEBOOK, APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/.

[19] FACEBOOK, RETARGETING, https://www.facebook.com/business/goals/retargeting.

29.   An example illustrates the point. Take an individual who navigates to one of Defendants' websites and clicks on a tab for allergy information. When that tab is clicked, the individual's browser sends a GET request to Defendants' server requesting that server to load the particular webpage. Because Defendants utilize the Facebook Tracking Pixel, Facebook's embedded code, written in JavaScript, sends secret instructions back to the individual's browser, without alerting the individual that this is happening. Facebook causes the browser to secretly and concurrently duplicate the communication with the Johns Hopkins website at issue, transmitting it to Facebook's servers, alongside additional information that transcribes the communication's content and the individual's identity.

30.   After collecting and intercepting this information, Facebook processes it, analyzes it and assimilates it into datasets like Core Audiences and Custom Audiences.

How Defendants Disclose Plaintiff's and Class Members' Protected Health Information and Assists with Intercepting Communications

31.   Through the Facebook Tracking Pixel, Defendants – via Johns Hopkins's websites – shares Johns Hopkins's patients' identities and online activity, including information and search results related to their private medical treatment.

32.   An investigation by *The Markup* revealed that thirty-three of the top 100 hospitals in the United States, as ranked by *Newsweek*, have the Facebook Tracking Pixel embedded on the appointment schedule pages of their websites, among other possible places.[20] Johns Hopkins is one of the identified websites.[21]

---

[20] Todd Feathers, *et al.*, FACEBOOK IS RECEIVING SENSITIVE MEDICAL INFORMATION FROM HOSPITAL WEBSITES, THE MARKUP ("Markup Investigation") (June 16, 2022), https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites.
[21] *Id.*

33.   According to the Markup Investigation, the hospital websites are "collecting patients' sensitive health information – including details about their medical conditions, prescriptions, and doctor's appointments – and sending it to Facebook."[22]

34.   The Markup Investigation further revealed that the data sent to Facebook is connected to: (a) the IP address of the computer sending the information, providing Facebook with the ability to connect the sensitive information to specific individual or household; or, worse: (b) a specific Facebook user if the user is logged into their Facebook account when using the websites at issue.[23]

35.   The Markup Investigation provided the following examples of the types of information surreptitiously intercepted by Facebook: (a) "clicking the 'Schedule Online' button on a doctor's page [of a specified hospital] prompted the [Facebook Tracking Pixel] to send Facebook the text of the button, the doctor's name, and the search term we used to find her: 'pregnancy termination'"; and (b) clicking the "Schedule Online Now' button on a different website "prompted the [Facebook Tracking Pixel] to send Facebook the text of the button, the doctor's name, and the condition we selected from the dropdown menu: "Alzheimer's."[24]

36.   The startling information revealed in the Markup Investigation prompted a former senior privacy advisor for the U.S. Department of Health and Human Services' Office for Civil Rights ("Office for Civil Rights") to remark on the troubling nature of the conduct: "I am deeply troubled by what [the hospitals] are doing with the capture of [patients'] data and the sharing of it."[25]
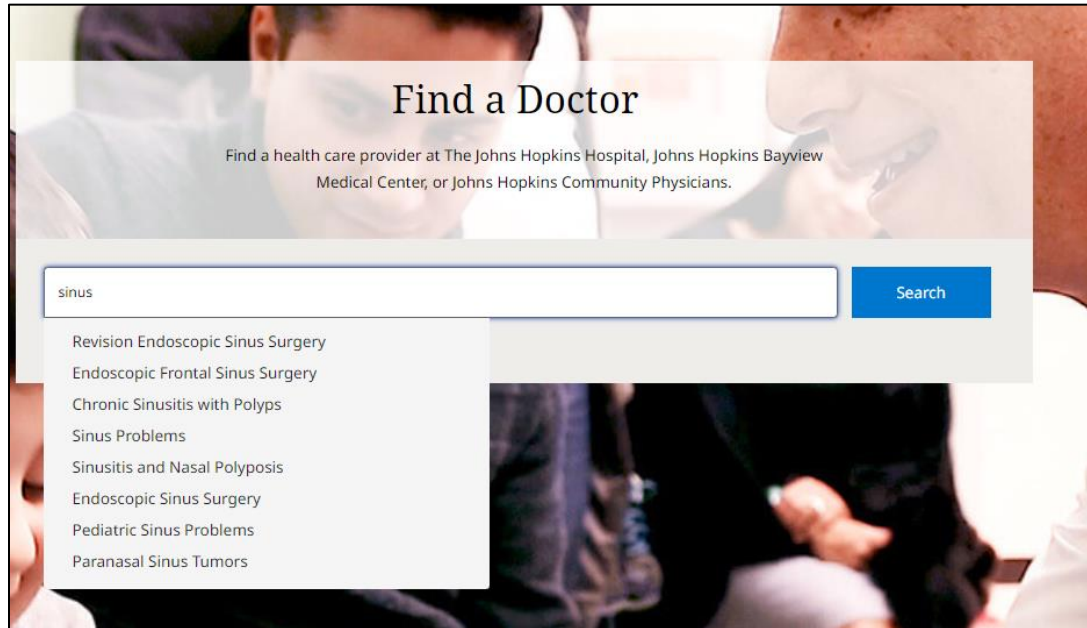
---

[22] *Id.*
[23] *Id.*
[24] *Id.*
[25] *Id.*

How Defendants Disclose Protected Health Information

37.   Defendants allow patients to select options like "Doctors," "Locations," "Appointments," and "MyChart."
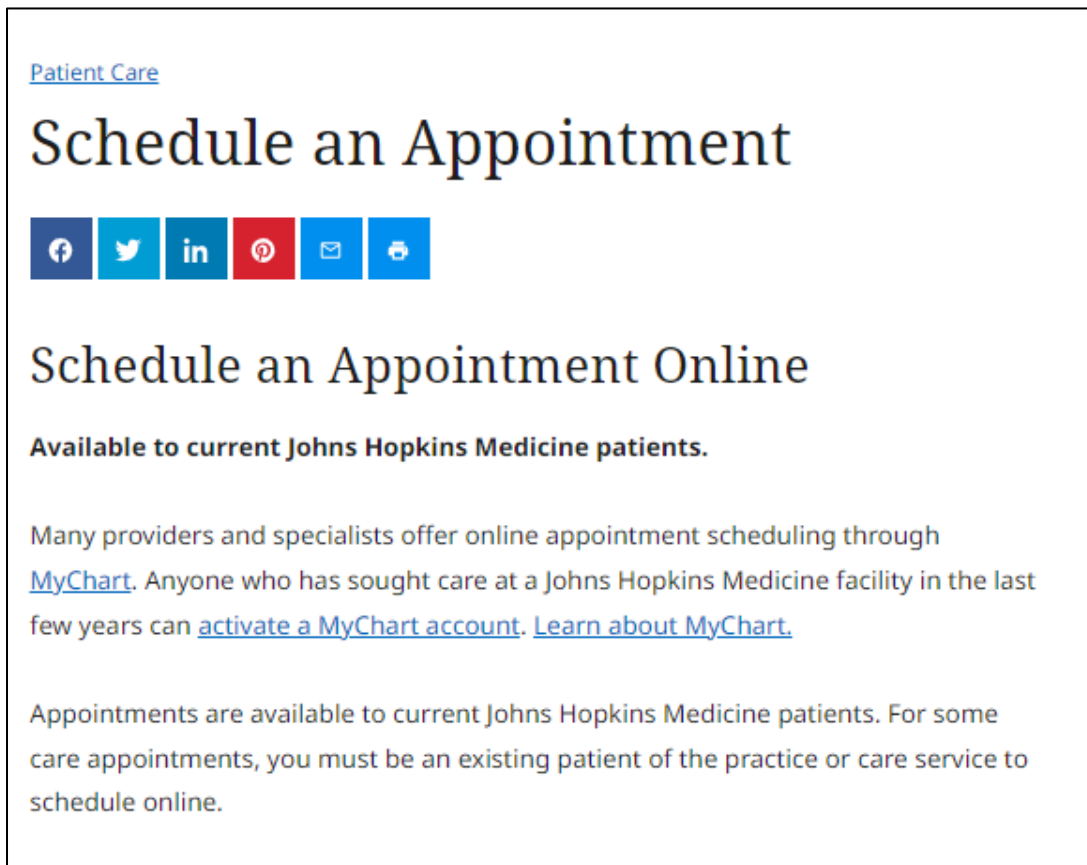
38.   When patients click "Doctors," they can search by "[l]ast name, speciality, or keyword."

39.   When patients click "Locations," they can search for Defendants' facilities.

40.   When patients click on "Appointments," they can access the protected portal.

41.   Upon information and belief, whenever patients search their treatment or condition, or whenever patients search Defendants' locations, Defendants procure Facebook to intercept communications that contain protected health information.

42.   Each time Defendants send this content, it also discloses a patient's personally identifiable information, including their Facebook ID ("FID"). An FID is a unique and persistent identifier that Facebook assigns to each user. With it, any ordinary person can look up the user's Facebook profile and name. Notably, while Facebook can easily identify any individual on its own Facebook platform with only their unique FID, so too can any ordinary person who comes into possession of an FID. Facebook admits as much on its website. Indeed, to find a

corresponding profile, a person need only attach the FID to the end of the URL for Facebook, typing in Facebook.com/[FID].

43.   A user who accesses Defendants' website while logged into Facebook will transmit what is known as the "c_user cookie" to Facebook, which contains that user's unencrypted Facebook ID.

44.   When a visitor's browser has recently logged out of an account, Facebook compels the visitor's browser to send a smaller set of cookies.

45.   One such cookie is the "fr cookie" which contains, at least, an unencrypted Facebook ID and browser identifier. Facebook, at a minimum, uses the fr cookie to identify users.[26]

46.   If a visitor has never created an account, an even small set of cookies are transmitted.

47.   At each stage, Defendants also utilize the "_fbp cookie," which attaches to a browser as a first-party cookie, and which Facebook uses to identify a browser and a user. [27]

48.   The fr cookie expires after 90 days unless the visitor's browser logs back into Facebook. [28]   If that happens, the time resets, and another 90 days begins to accrue. [29]

---

[26] FACEBOOK, COOKIES & OTHER STORAGE TECHNOLOGIES,
https://www.facebook.com/policy/cookies/.
[27] FACEBOOK, COOKIES & OTHER STORAGE TECHNOLOGIES,
https://www.facebook.com/policy/cookies/.
[28] *See* FACEBOOK, COOKIES & OTHER STORAGE TECHNOLOGIES,
https://www.facebook.com/policy/cookies/.
[29] Confirmable through developer tools.

49.   The _fbp cookie expires after 90 days unless the visitor's browser accesses the same website. [30] If that happens, the time rests, and another 90 days begins to accrue. [31]

50.   The Facebook Pixel uses both first- and third-party cookies. A first-party cookie is "created by the website the user is visiting"—*i.e.*, Johns Hopkins. [32] A third-party cookie is "created by a website with a domain name other than the one the user is currently visiting"—*i.e.*, Facebook. [33] The _fbp cookie is always transmitted as a first-party cookie. A duplicate _fbp cookie is sometimes sent as a third-party cookie, depending on whether the browser has recently logged into Facebook.

51.   Facebook, at a minimum, uses the fr, _fbp, and c_user cookies to link to Facebook IDs and corresponding Facebook profiles. Defendants send these identifiers alongside the event data.

52.   Plaintiff never consented, agreed, or otherwise permitted Defendants to disclose their personally identifiable information and protected health information. Plaintiff was never provided with any written notice that Defendants disclosed their users' protected health information, nor were they provided any means of opting out of such disclosures. Defendants nonetheless knowingly disclosed Plaintiff's protected health information to Facebook.

53.   By law, Plaintiff is entitled to privacy in their protected health information and confidential communications. Defendants deprived Plaintiff of her privacy rights by procuring

---

[30] *See* FACEBOOK, COOKIES & OTHER STORAGE TECHNOLOGIES, https://www.facebook.com/policy/cookies/.
[31] Also confirmable through developer tools.
[32] PC MAG, FIRST-PARTY COOKIES, https://www.pcmag.com/encyclopedia/term/first-party-cookie. This is confirmable by using developer tools to inspect a website's cookies and track network activity.
[33] PC MAG, THIRD-PARTY COOKIES, https://www.pcmag.com/encyclopedia/term/third-party-cookie. This is also confirmable by tracking network activity.

Facebook to intercept these communications by implementing a system that surreptitiously tracked, recorded, and disclosed Plaintiff's and other patients' confidential communications, personally identifiable information, and protected health information. Plaintiff did not discover that Defendants disclosed her personally identifiable information and protected health information to Facebook, and assisted Facebook with intercepting their communications, until January 2023.

The Expectation of Privacy in Healthcare Information

54.   An individual's medical records and information are among the most sensitive type of personal information.

55.   Indeed, the State requires that medical records be treated as confidential. Md. Code Cts. & Jud. Proc. § 10-410.

56.   Similarly, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") imposes strict standards to protect sensitive patient health information from being disclosed without the patients' knowledge and consent. *See* 45 C.F.R. § 160, *et seq.*

57.   On December 1, 2022, the Office for Civil Rights issued a bulletin titled *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* (the "Bulletin") in which it addressed the impropriety of healthcare providers utilizing tracking technologies such as the Facebook Tracking Pixel in a manner that impermissibly discloses protected health information ("PHI") in violation of the HIPAA.[34]

58.   According to the Office for Civil Rights, "**[r]egulated entities** [those to which HIPAA applies] **are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of [protected health information] to tracking technology**

---

[34] U.S. Dep't of Health and Human Services – Office for Civil Rights, Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates (Dec. 1, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

vendors or any other violations of the HIPAA Rules."[35] As set forth in the Bulletin, "disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures."[36]

59.   Outside of HIPAA, the Office for Civil Rights warned that an impermissible disclosure of an individual's PHI could result in a wide range of additional harms to the individual or others.[37] "For example, an impermissible disclosure of PHI may result in identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or others identified in the individual's PHI."[38]

60.   The Office for Civil Rights noted the broad range of information that constitutes PHI, including "individually identifiable health information" ("IIHI") such as "an individual's medical record number, home or email address, or dates of appointments, as well as an individual's IP address or geographic location, medical device IDs, or any unique identifying code."[39] According to the Bulletin, IIHI can constitute PHI because:

> when a regulated entity collects the individual's IIHI through its website or mobile app, the information connects the individual to the regulated entity (*i.e.*, it is indicative that the individual has received or will receive health care services or benefits from the covered entity), and thus relates to the individual's past, present, or future health or health care or payment for care.[40]

---

[35] *Id.* (emphasis in original).
[36] *Id.*
[37] *Id.*
[38] *Id.*
[39] *Id.*
[40] *Id.*

61.   The Office for Civil Rights concluded that "it is critical for regulated entities to ensure that they disclose PHI **only** as expressly permitted or required by the HIPAA Privacy Rule."[41]

62.   As a result of Defendants' conduct, as alleged herein, Plaintiff and Class Members have been exposed to the harms and impending harms described in the Bulletin.

63.   Moreover, "courts have recognized the 'growing trend across courts . . . to recognize the lost property value' of personal information. *In re Marriott Int'l, Inc., Cust. Data Sec. Breach Litig.*, 440 F.Supp.3d 447, 461 (D. Md. 2020) . . .; *see also In re Facebook Privacy Litigation*, 557 F.App'x. 494, 494 [sic] (9th Cir. 2014)." *Calhoun v. Google LLC*, 526 F.Supp.3d 605, 636 (N.D. Cal. 2021).

CLASS ACTION ALLEGATIONS

64.   Plaintiff pursuant to Rule 2-231 of the Maryland Rules of Civil Procedure, asserts this action individually and on behalf of the following Class: All natural persons in Maryland whose personal information was collected through the Facebook Tracking Pixel.

65.   Plaintiff reserves the right to amend or modify the Class definition with greater specificity or division and/or to add subclasses after having had an opportunity to conduct discovery.

66.   Excluded from the Class are: (a) Defendants; (b) any parent, affiliate or subsidiary of Defendants; (c) any entity in which Defendants have a controlling interest; (d) any of Defendants' officers or directors; (e) any successor or assign of Defendants; (f) any judge or court personnel assigned to this case and members of their immediate families; and (g) Plaintiff's counsel and Defendants' counsel and anyone employed by them.

---

[41] *Id.* (emphasis in original).

67.   **Numerosity.** Consistent with Maryland Rule of Civil Procedure Rule 2-231(b), the

Class is so numerous that joinder of all members is impracticable. While Plaintiff does not know

the exact number of members of the Class, Plaintiff believes the Class contains at least hundreds

of thousands of individuals, and the members can be identified through Defendants' records. Class

Members may be notified of the pendency of this action by recognized, Court-approved notice

dissemination methods, which may include U.S. mail, electronic mail, internet postings, social

media and/or published notice.

68.   **Commonality.** Common questions of law and fact exist as to all Class Members.

These common questions of law or fact predominate over any questions affecting only individual

members of the Class. Common questions include, but are not limited to the following:

a. Whether Plaintiff and Class Members had a reasonable expectation of privacy in their sensitive health information communicated to their healthcare providers;

b. Whether Defendants violated Plaintiff's and Class Members' privacy rights;

c. Whether Defendants intentionally tapped the lines of internet communication between Plaintiff and Class Members and their medical providers;

d. Whether Defendants' website surreptitiously record personally identifiable information, protected health information and related communications and simultaneously, or subsequently, discloses that information to Facebook.

e. Whether Defendants procured Facebook to intercept communications;

f. Whether Defendants' disclosure of personally identifiable information, protected health information and related communications constitutes an affirmative act of communication;

g. Whether Defendants' actions violated the Maryland Wiretap Act; and

19

> h. Whether Plaintiff's and Class Members are entitled to damages under the Maryland Wiretap Act.

69. **Typicality.** Plaintiff's claims are typical of the claims of the Class she seeks to represent because Plaintiff and all Class Members have suffered similar injuries as a result of the same practices alleged herein. Plaintiff has no interests to advance adverse to the interests of the other Class Members, and Defendants have no defenses unique to any Plaintiff.

70. **Adequate Representation.** Plaintiff has and will continue to fairly and adequately represent and protect the interests of the Class and have retained as her counsel attorneys competent and experienced in class actions and complex litigation, including litigation to remedy privacy violations. Plaintiff and her counsel are committed to vigorously prosecuting this action on behalf of Class Members, and they have the resources to do so.

71. **Predominance.** Common questions of law and fact predominate over any questions affecting only individual class members. For example, Defendants' liability and the fact of damages is common to all members of the Class.

72. **Superiority and Manageability.** A class action is superior to other available means for the fair and efficient adjudication of this dispute. The injury suffered by each Class Member, while meaningful on an individual basis, may not be of such magnitude as to make the prosecution of individual actions against Defendants economically feasible. Even if Class Members could afford individual litigation, those actions would put immeasurable strain on the court system. Moreover, individual litigation of the legal and factual issues of the case would increase the delay and expense to all parties and the court system. A class action, however, presents far fewer management difficulties and provides the benefit of single adjudication, economy of scale and comprehensive supervision by a single court.

73.   **Risk of Inconsistent, Varying, or Prejudicial Adjudications.** A class action will minimize the risk of inconsistent, varying or prejudicial adjudications. If Plaintiff's and Class Members' claims were tried separately, Defendants would be confronted with incompatible standards of conduct and divergent court decisions.

CLAIMS FOR RELIEF

COUNT I
Violation of the Maryland Wiretap Act
18 Pa. Cons. Stat. § 5701, *et seq.*

74.   Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein.

75.   Plaintiff brings this Count individually and on behalf of the members of the Class.

76.   Maryland's Wiretap Act prohibits: (a) the interception or procurement of another to intercept any wire, electronic or oral communication; (b) the intentional disclosure of the contents of any wire, electronic or oral communication that the discloser knew or should have known was obtained through the interception of a wire, electronic or oral communication; and (c) the intentional use of the contents of any wire, electronic or oral communication that the discloser knew or should have known was obtained through the interception of a wire, electronic or oral communication. Md. Cts. & Jud. Proc. Code § 10-402.

77.   Any person who intercepts, discloses, or uses or procures any other person to intercept, disclose or use, a wire, electronic, or oral communication in violation of the Maryland's Wiretap Act is subject to a civil action for: (a) actual damages, not less than liquidated damages computed at the rate of $100/day for each violation or $1,000, whichever is higher; (b) punitive damages; and (c) reasonable attorneys' fees and other litigation costs incurred. Md. Cts. & Jud. Proc. Code § 10-410.

78.   At all relevant times, Defendants procured Facebook to track and intercept Plaintiff's and Class members' internet communications while navigating www.hopkinsmedicine.org. They intercepted these communications without authorization and consent from Plaintiff and Class members.

79.   Defendants, when procuring Facebook to intercept Plaintiff's communications, intended Facebook to learn the meaning of the content the visitor requested.

80.   Plaintiff and Class members had a justified expectation under the circumstances that their electronic communications would not be intercepted.

81.   Plaintiff and Class members were not aware that their electronic communications were being intercepted by Facebook.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seeks judgment against Defendants, as follows:

a.   Determining that this action is a proper class action;

b.   For an order certifying the Class, naming Plaintiff as representative of the Class, and naming Plaintiff's attorneys as Class Counsel to represent the Class;

c.   For an order declaring that Defendants' conduct violates the statute referenced herein;

d.   For an order finding in favor of Plaintiff and the Class on the count asserted herein;

e.   Award compensatory damages, including statutory damages where available, to Plaintiff and the Class members against Defendants, jointly and severally, for all damages sustained as a result of Defendants' wrongdoing, in an amount to be proven at trial;

f.   For punitive damages, as warranted, in an amount to be determined at trial;

g.   Ordering Defendants to disgorge revenues and profits wrongfully obtained;

h.   For prejudgment interest on all amounts awarded;

i.   For injunctive relief as pleaded or as the Court may deem proper;

j.   For an order awarding Plaintiff and the Class their reasonable attorneys' fees and

expenses and costs of suit; and

k.   Grant Plaintiff and the Class members such further relief as the Court deems

appropriate.

JURY DEMAND

Plaintiff hereby demands a trial by jury on all claims so triable in this action.

Dated: February 3, 2023   Respectfully submitted,

MANN & RISCH LLC

/s/ Nathaniel K. Risch
Nathaniel K. Risch
AIS: 0612130253
101 E. Chesapeake Ave., Ste. 403
Towson, MD 21286
Tel: (410) 929-5145
Fax: (410) 307-1007
E-Mail: nate@mannrisch.com

BURSOR & FISHER, P.A.
Joshua D. Arisohn*
Philip L. Fraietta*
888 Seventh Avenue
New York, NY 10019
Tel: (646) 837-7150
Fax: (212) 989-9163
E-Mail: jarisohn@bursor.com
            pfraietta@bursor.com

BURSOR & FISHER, P.A.
Christopher R. Reilly*
701 Brickell Ave., Suite 1420
Miami, FL 33131-2800
Telephone: (305) 330-5512
Facsimile: (305) 676-9006
E-Mail: creilly@bursor.com

DRURY LEGAL, LLC
Scott R. Drury*
6 Carriage Lane
Highwood, Illinois 60040
Telephone: (312) 358-8225
E-Mail: scott@drurylegal.com

Pro Hac Vice Application Forthcoming

Attorneys for Plaintiff and the Putative Class

24